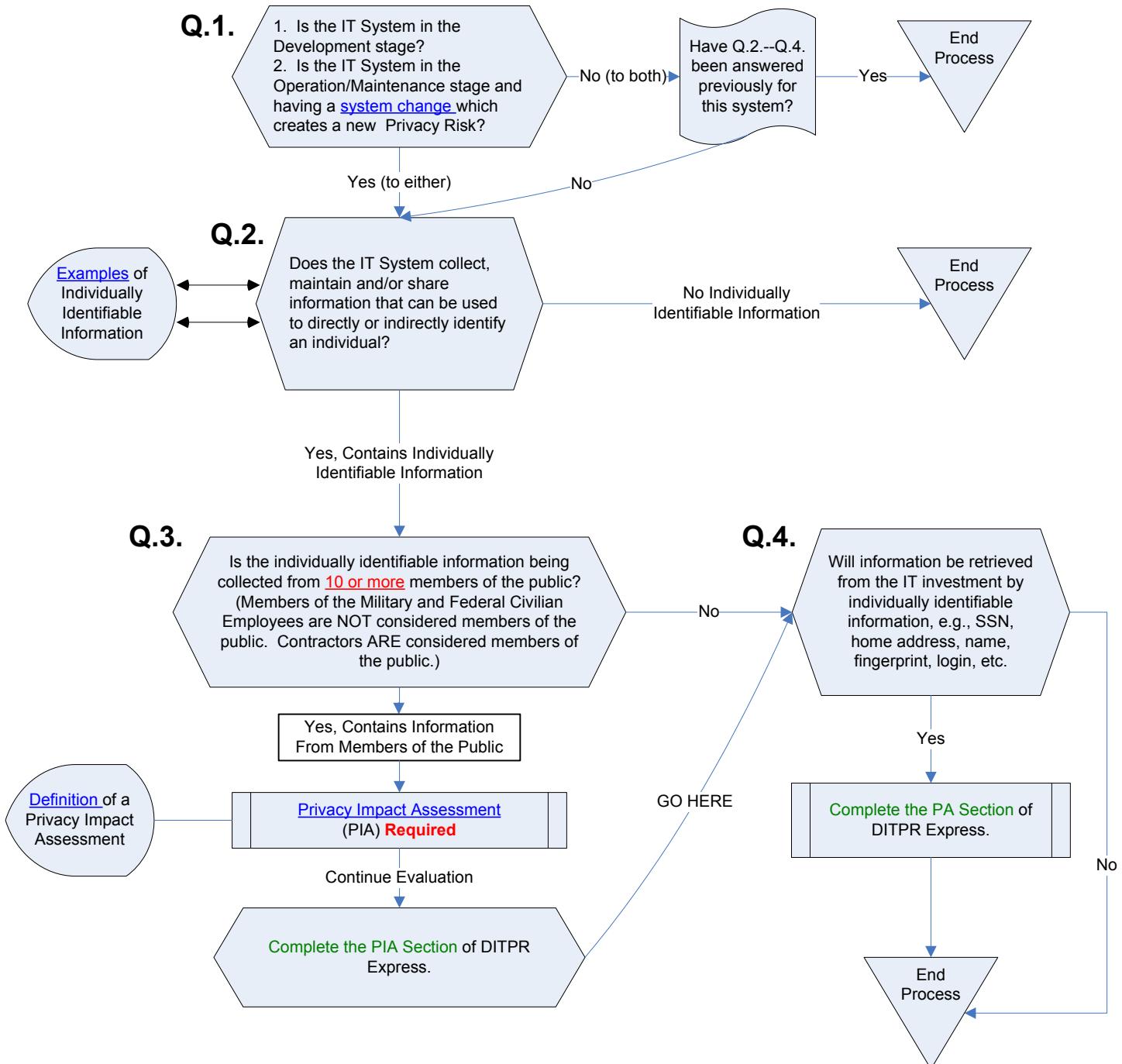


Do you need to complete this section of DITPR Express?



Examples of Individually Identifiable Information From the E-Gov Act's Legislative History

Examples¹ of Individually Identifiable Information:

- a first and last name;
- a home or other physical address;
- an e-mail address;
- a telephone number;
- a social security number;
- a credit card number;
- a birth date, birth certificate number, or a place of birth.

Note 1: See section 208(b)(1)(A)(ii)(II) from page 29 of Senate Report 107-174 to accompany S.803, "E-GOVERNMENT ACT OF 2001," 24 June 2002.

- computer device number
- in general, any data element that points to a specific person

[Return to
Main Diagram](#)

Examples of System Changes From the E-Gov Act

[Return to Main Diagram](#)

- a. **Conversions** - when converting paper-based records to electronic systems;
- b. **Anonymous to Non-Anonymous** - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- c. **Significant System Management Changes** - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
 - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
- d. **Significant Merging** - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
 - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
- e. **New Public Access** - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- f. **Commercial Sources** - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

More Examples of System Changes From the E-Gov Act

- g. **New Interagency Uses** - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
 - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.
- h. **Internal Flow or Collection** - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
 - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
- i. **Alteration in Character of Data** - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

[Return to Main Diagram](#)

Definition of a Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how individually identifiable information is collected, stored, protected, shared and managed. A PIA should demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. This involves making certain that privacy protections are built into the system from the start, not after the fact when they can be far more costly or could affect the viability of the project.

[Return to
Main Diagram](#)